Aufgabe H12T1A5 (3+2 Punkte)

(a) Die Anzahl der Tänzer in einem Ballsaal liegt zwischen 100 und 200. Stellt man sie in 11-er Reihen auf, so bleibt ein Tänzer allein. Stellt man sie dagegen in 5-er Reihen auf, so bleiben drei übrig. Und stellt man sie in 3-er Reihen auf, so bleiben zwei Tänzer allein. Wieviele Tänzer sind es genau?

(b) Geben Sie explizit einen Ring-Isomorphismus

$$\varphi : \mathbb{Z}/57\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$$

und seine Umkehrung φ^{-1} an.

Lösung:

zu (a) Sei x die Anzahl der Tänzer in dem Ballsaal. Laut Angabe gilt $100 \leq x \leq 200$. Die Aufstellung in 11-er Reihen liefert uns die Bedingung $x \equiv 1 \bmod 11$. Daraus folgt, dass es sich bei x um eine der Zahlen

$$100 \ , \ 111 \ , \ 122 \ , \ 133 \ , \ 144 \ , \ 155 \ , \ 166 \ , \ 177 \ , \ 188 \ , \ 199$$

Entsprechend liefern uns die anderen beiden Aufstellungen die Kongruenzen $x \equiv 3 \bmod 5$ und $x \equiv 2 \bmod 3$. Die Kongruenz modulo 5 lässt aus der Liste nur die Zahlen zu, deren letzte Dezimalstelle eine 3 oder eine 8 ist, also 133 oder 188. Es gilt $133 \equiv 13 \equiv 1 \bmod 3$ und $188 \equiv 38 \equiv 2 \bmod 3$. Also zeigt die Kongruenz modulo 3, dass 188 die gesuchte Anzahl ist.

zu (b) Als verschiedene Primzahlen sind 3 und 19 teilerfremd. Laut Chinesischem Restsatz gibt es deshalb einen eindeutig bestimmten Isomorphismus von Ringen $\varphi : \mathbb{Z}/57\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$ mit $\varphi(a+57\mathbb{Z}) = (a+3\mathbb{Z}, a+19\mathbb{Z})$ für alle $a \in Z$. In der Vorlesung wurde ein Verfahren zur Bestimmung der Umkehrabbildung von φ behandelt. Zunächst verwenden wir den Euklidischen Algorithmus, um ganze Zahlen x, y mit $3x + 19y = \mathrm{ggT}(3, 19) = 1$ zu bestimmen.

q	a_n	x_n	y_n
$--$	19	1	0
$--$	3	0	1
6	1	1	-6
3	0	$--$	$--$

An der vorletzten Zeile kann abgelesen werden, das die oben angegebene Gleichung mit $x = -6$ und $y = 1$ erfüllt ist, d.h. es gilt $3 \cdot (-6) + 19 \cdot 1 = 1$. Die umgestellte Gleichung $1 + 3 \cdot 6 = 1 \cdot 19$ zeigt, dass $\varphi(19 + 57\mathbb{Z}) = (1 + 3\mathbb{Z}, 0 + 19\mathbb{Z})$ gilt. An der Gleichung $3 \cdot (-6) = -18 = 1 + 19 \cdot (-1)$ liest man dass $\varphi(-18+57\mathbb{Z}) = (0+3\mathbb{Z}, 1+19\mathbb{Z})$ ab. Für alle $a, b \in \mathbb{Z}$ gilt somit $\varphi(19a-18b+57\mathbb{Z}) = (a+3\mathbb{Z}, b+19\mathbb{Z})$. Die Umkehrabbildung von φ ist also geben durch

$$\varphi^{-1}(a + 3\mathbb{Z}, b + 19\mathbb{Z}) \quad = \quad 19a - 18b + 57\mathbb{Z}.$$

Beispielsweise ist $\varphi^{-1}(2 + 3\mathbb{Z}, 7 + 19\mathbb{Z}) = (19 \cdot 2 - 18 \cdot 7) + 57\mathbb{Z} = -88 + 57\mathbb{Z} = 26 + 57\mathbb{Z}$.